UNITED STATES DISTRICT COURT

DISTRICT OF SOUTH DAKOTA

SOUTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. JEREMY VINCENT NELSON, Defendant.	)))))))))	CR. 09-40130-01-KES ORDER ADOPTING REPORT AND RECOMMENDATION

Defendant, Jeremy Vincent Nelson, is charged with one count of possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2256(8). Nelson moves to suppress evidence obtained during a search of his residence and vehicle on or about November 4, 2009, and for a Franks hearing. The court referred Nelson's motion to Magistrate Judge John E. Simko pursuant to 28 U.S.C. § 636(b)(1)(B). After holding an evidentiary hearing, Magistrate Judge Simko recommended that this court grant Nelson's motion to suppress and for a Franks hearing. The government objects to nine of Magistrate Judge Simko's factual and legal findings. Nelson has no objection to Magistrate Judge Simko's report and recommendation. After a de novo review of the report and recommendation and a review of the record, the court adopts the report and recommendation and grants Nelson's motion to suppress and for a Franks hearing.

STANDARD OF REVIEW

Under 28 U.S.C. § 636(b)(1), "when a party objects to the report and recommendation of a magistrate judge concerning a dispositive matter, '[a] judge of the court shall make a de novo determination of those portions of the report or specified proposed findings or recommendations to which objection is made.' " United States v. Lothridge, 324 F.3d 599, 600 (8th Cir. 2003) (quoting 28 U.S.C. § 636(b)(1)); see also Fed. R. Civ. P. 72(b) ("The district judge must determine de novo any part of the magistrate judge's disposition that has been properly objected to.").

BACKGROUND

Troy Boone is the Task Force Commander for the State of South Dakota Internet Crimes Against Children Task Force. On September 27, 2009, Agent Boone came across an IP address that was distributing files known to be child pornography. Agent Boone identified the files as child pornography by comparing the hash values of the files to the hash values of known child pornography. When two files have the same hash value, there is a 99.99 percent chance that they are the same file. The IP address distributing child pornography files was 216.16.82.227.

Agent Boone kept track of the file-sharing activity conducted by IP address 216.16.82.227 from September 29, 2009, to October 31, 2009. This activity was recorded in a 79-page log, the first page of which was introduced

into evidence as Exhibit 6. Exhibit 6 indicates that the port number associated with the file-sharing activity was 22662, meaning that the subscriber using IP address 216.16.82.227 to access the Internet was using the channel identified as port number 22662 to communicate with file-sharing software. Agent Boone testified that the port number was 22662 during the entire 33-day period for which he tracked the file-sharing activity conducted by IP address 216.16.82.227. Agent Boone also testified that the port number is never the same from computer to computer and that if the same port number is associated with the same IP address over a certain period, then it was probably the same computer the whole time. Agent Boone had the IP history and port number for IP address 216.16.82.227 at the time he prepared the affidavit in support of the search warrant in question in this case.

In the course of his investigation, Agent Boone also obtained and served a subpoena on Knology, an Internet service provider, requesting "[s]ubscriber information for IP address 216.16.82.227 on 9-28-09 at 00:46 (+0000) GMT to 9-28-09 at 00:29 (+0000) GMT, including any and all billing information and payment information including credit card number, connection dates and times, and current IP address." Exhibit 4.[1] The parties agree that the times on the subpoena were reversed, so that the subpoena should have read "9-28-09

[1] "GMT" refers to Greenwich Mean Time. Central Daylight Time, the time zone applicable at the times and places relevant to this case, is five hours behind Greenwich Mean Time.

at 00:29 (+0000) GMT to 9-28-09 at 00:46 (+0000) GMT." Converted into Central Daylight Time (CDT), the subpoena requested subscriber information for IP address 216.16.82.227 for 7:29 p.m. to 7:46 p.m. on September 27, 2009. In response to this subpoena, Knology sent a series of emails to Agent Boone. These emails were introduced into evidence as Exhibit 2.

The series of emails shows that on September 30, 2009, Jason Griggs, Knology's Security and Fraud Coordinator and Subpoena and Legal Compliance Officer, contacted David Johnson, another Knology employee, and stated that he needed Dynamic Host Control Protocol (DHCP) logs and subscriber information for IP address 216.16.82.227 from September 28, 2009, through the most current date. Exhibit 2 at 7.[2] Johnson replied on October 5, 2009, that he could not determine the modem and/or account information for

[2] Daryl Elcock, network manager for the Sioux Falls division of Knology, explained the meaning of various technical terms at the evidentiary hearing. To access the Internet via a cable modem and Knology's network, a personal computer or router must connect to the cable modem, which in turn makes a request to get on the Knology network. The cable modem is then given an "Internet Protocol (IP) address" that completes the connection between the cable modem and the Knology network. The IP address is assigned at and through the DHCP, which keeps a log of connections to and access to an IP address. There are several layers of communication between the cable modem and the DHCP server and the personal computer and the DHCP server. A "DHCP log" refers to a log of these connections and communications.

Every cable modem, personal computer, and server that wants to access the Internet or network has a "MAC address," which is a unique identifier for that piece of equipment. The MAC address is attached to the network interface card on the device.

that IP address. Id. at 7. That day, Griggs asked Johnson if the subscriber could have disconnected service. Id. at 6-7. Johnson stated that he had consulted Cynthia Spence, another Knology employee, and Spence theorized that the DHCP log showed two MAC addresses slammed together. Id. at 6. Griggs asked Johnson to keep trying to locate the customer. Id. at 5.

On October 7, 2009, Spence sent an email to Jason Rang, a Knology employee, which said: "[h]ere is what DHCP spit out when we queried it on the date in question for the user of the IP address." Id. at 3. Spence copied a DHCP log for September 28, 2009, into this email. Id. at 4-5. The September 28, 2009, log reflects activity by IP address 216.16.82.227 and a computer with MAC address 00:1e:ec:2e:cc:36 as well as a device with MAC address 00:19:b9:de:7d:c3:00:0a:8b:19:70:0a:08:00. The time of the activity was between 11:24:19 p.m. CDT and 11:24:22 p.m. CDT. Rang replied that it looked like an IPV6 MAC address or a spoofed address and asked whether law enforcement could provide a MAC address to see if it matched the 00:1e:ec:2e:cc:36 address. Id. at 3. Spence then asked Griggs if the police had a suspected MAC address, and Griggs indicated that the police were looking to Knology to uncover that information. Id. at 2-3. Spence replied that they would "just have to keep monitoring and hope [the subscriber] gets online." Id. at 2. She also asked Griggs to "let the police know that we need to know ASAP

if [the subscriber] sends out more material so we can check our logs again." Id. at 2.

On October 8, 2009, Griggs emailed Agent Boone. Griggs informed Agent Boone that Knology was still working to determine the subscriber information for IP address 216.16.82.227, but that it appeared that the subscriber had not been online since September 28, 2009. Griggs suggested that the subscriber had unplugged his modem or was using a spoofed IP address. Griggs also indicated that Knology technicians had recorded the subscriber's home computer MAC address as 00:1e:ec:2e:cc:36 and were keeping an eye out for it. Finally, Griggs asked Agent Boone to notify him immediately if the subscriber started his activity again. Id. at 1. It is unclear from Exhibit 2 whether Griggs forwarded the previous chain of emails to Agent Boone at this time. Agent Boone testified that he received some of the emails on this day. Agent Boone replied to Griggs on October 9, 2009, saying that he had seen the subscriber on the system "on 10-6-09 @ 1307 (+0000), 10-5-09 @ 10:59 (+0000), 10-3-09 @ 00:51 (+0000)." Id. at 1. Agent Boone also informed Griggs that he had captured that the subscriber was using port number 22662 for file-sharing software. Id.

Finally, on October 12, 2009, Griggs sent Agent Boone an email saying, "[h]ere is the info for the IP address '216.16.82.227' for the date of 10/06/2009. The same user is assigned the same IP address today (also

included in the log)." Id. at 1. Griggs attached a document containing Nelson's subscriber information and DHCP logs for IP address 216.16.82.227 on October 6, 2009, and October 12, 2009, to this email. The attachment, which was introduced into evidence as Exhibit 7, does not include DHCP logs for September 28, 2009. Agent Boone received the entire chain of emails in Exhibit 2 on October 12, 2009.

On November 2, 2009, Agent Boone created an affidavit in support of a request for a search warrant for Nelson's residence at 616½ Locust St., Yankton, SD 57078. See Exhibit 5. Agent Boone described his background in investigating child pornography offenses and stated,

> [o]n September 28, 2009, . . . I was able to identify a computer at an IP address that appeared to be offering files consistent with child pornography for distribution. This can be done as IP addresses are often a temporary number issued to a computer on a network and after the IP address is no longer in use, it is reassigned to another computer. This is illustrated by having to subpoena an Internet Service Provider for an exact date/time pertaining to an IP address for an investigation.

Id. at NELSON-0026. Agent Boone further stated that the "IP address that was offering files consistent with child pornography for distribution was 216.16.82.227 on 9-28-09 at 00:46AM GMT (+0000)." Id. at NELSON-0027. Agent Boone attested that he conducted an IP history check and obtained an IP history for IP address 216.16.82.227 that indicated the dates, times, file names, IP address, port number, and hash value for the known or suspected images consistent with child pornography that were seen on file-sharing

software at that IP address. Id. Agent Boone also stated that he used the American Registry for Internet Numbers and learned that the IP address was issued to Knology in Yankton, South Dakota. Id.

Then, Agent Boone explained, "[o]n September 30, 2009, I served legal process to Knology for the IP address 216.16.82.227 at the dates and times provided to me by the Wyoming ICAC database for the images consistent with child pornography being offered for distribution on the Gnutella network." Id. And in the paragraph at issue in this case, Agent Boone stated, "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested." Id. Agent Boone then described the content of several files he observed in the IP history for IP address 216.16.82.227. Id. at NELSON-0027 to -0028. The affidavit does not mention port numbers or MAC addresses or discuss the relationship between a MAC address and an IP address.

Both Agent Boone and Daryl Elcock, network manager for the Sioux Falls division of Knology, testified at length at the evidentiary hearing about the content of the DHCP logs for IP address 216.16.82.227.[3] Agent Boone and

[3] The relevant DHCP logs were introduced into evidence in various forms. As noted, the September 28, 2009, DHCP logs were copied into Spence's October 7, 2009, email to Rang. See Exhibit 2 at 4-5. The October 6, 2009, and October 12, 2009, DHCP logs (as well as Nelson's subscriber information) were attached to Griggs's October 12, 2009, email to Agent Boone. See

Elcock testified that the subscriber information for IP address 216.16.82.227 could be determined from the DHCP logs by tracing the MAC addresses of the host modem and the personal computer associated with this IP address. The IP address 216.16.82.227 appears in the DHCP logs for September 28, 2009, October 6, 2009, and October 12, 2009. Exhibit 2 at 4; Exhibit 7. Further, the October 6, 2009, and October 12, 2009, DHCP logs indicate that the host modem had MAC address 00:1E:46:BE:D3:EC. See Exhibit 7. This means that the DHCP logs recorded the activity of the modem with this MAC address as well as the computer that accessed the Internet via this modem. Knology identified Nelson as the subscriber using a cable modem with MAC address 00:1E:46:BE:D3:EC. Id. Finally, the MAC address for the subscriber's computer, 00:1e:ec:2e:cc:36, appears under the heading, "[t]he DHCP logs

---

Exhibit 7. The government also introduced Exhibit 1, which combines into a single document Nelson's subscriber information and the DHCP logs for September 28, 2009, October 6, 2009, and October 12, 2009. Exhibit 1 was created by Knology for the purposes of responding to the subpoena, but it is unclear whether Knology provided a copy of Exhibit 1 to Agent Boone before Agent Boone executed the affidavit or whether Agent Boone had only the DHCP logs included in or attached to the relevant emails at that time. Indeed, the "Certification of Business Records" signed by Griggs and attached to Exhibit 1 is dated March 22, 2010. In any event, the DHCP logs in Exhibit 1 appear to contain the same data as the DHCP logs included in Knology's emails. The government also introduced Exhibit 3, which is an exact copy of Exhibit 1 with color-coded highlighting provided by the government. In order to ensure that the court examines only the information available to Agent Boone at the time he created the affidavit, the court will refer to the DHCP logs contained in and attached to Knology's emails. See Exhibit 2 at 4-5 (containing September 28, 2009, DHCP log); Exhibit 7 (containing subscriber information for Nelson and DHCP logs for October 6, 2009, and October 12, 2009).

show the following modem host," on Exhibit 7. The same MAC address appears in the DHCP logs for September 28, 2009, October 6, 2009, and October 12, 2009. Exhibit 2 at 4; Exhibit 7.[4] Elcock testified that he could tell from the DHCP logs for September 28, 2009, and October 6, 2009, that the same computer used the same modem on both dates.

The key issue in this case is whether Agent Boone's statement in the affidavit that "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON . . . on the dates and times requested," was false. Agent Boone repeatedly testified that the basis for this statement was his analysis of the information Knology sent him in the email chain, including the DHCP logs, as well as the results of the IP history he gathered in the case. For example, Agent Boone testified, "[b]ased on what Knology had sent me in the e-mail and the log file, and based on . . . the IP history that I used for this case, I knew that there was only one computer that would be responsible for the distribution of the child pornography images in this case." Tr. 35-36. He further explained,

> [b]ased on the . . . DHCP log that contained the MAC address of the modem, the MAC address of the computer, and based on the IP history that I had run through the Wyoming database, I knew that

[4] A third MAC address, 00:19:b9:de:7d:c3:00:0a:8b:19:70:0a:08:00, also appears on the DHCP log for September 28, 2009. Exhibit 2 at 4. Agent Boone testified that this MAC address did not have any significance in identifying the subscriber associated with IP address 216.16.82.227. Elcock could not identify or explain this MAC address.

> that particular computer was sharing child pornography at one IP address and at one port number, and sharing the same files over that 15 days time stretch from when I initially saw it to when I got the final Subpoena results back from Knology.

Tr. 36. Agent Boone later stated that the combination of the information in the email chain from Knology (Exhibit 2) and the attachment to the last email in that chain (Exhibit 7) "and also the IP history, and me looking at what that IP address had been doing on the Wyoming network" led him to write the challenged paragraph. Tr. 42. See also Tr. 59 (testifying that he identified Nelson as the person with the IP address 216.16.82.227 "[b]ased on this particular log [Exhibit 7], based on the e-mails, and then based on the IP history."). Agent Boone explained, "I looked at the e-mail, and if the two MAC addresses are identical and it's on September 28, October 6, October 12, and whatever other day we want to pick, and those two MAC addresses are the same to the same IP address, it has to be the same modem and the same computer." Tr. 78.

Magistrate Judge Simko asked Agent Boone, "Do I understand correctly that they [Knology] provided you information from which you figured out that Jeremy Nelson was the person, or did they tell you the person is Jeremy Nelson?" Tr. 36-37. Agent Boone responded, "I used the logs, the DHCP logs [Knology] sent me, and the other information that I had in my investigation and put them together to find out that it was Jeremy Nelson at this address." Tr. 37. Agent Boone later admitted that Knology never stated in a single sentence

that Nelson subscribed to IP address 216.16.82.227 on September 28, 2009. Tr. 78. He testified that it would have been more accurate to state that Knology "responded with information *indicating*" that IP address 216.16.82.227 was subscribed to by Nelson on the dates and times requested rather than Knology "responded with information *stating*" as such. Tr. 77 (emphasis added).

A search warrant was issued for Nelson's residence on the basis of Agent Boone's affidavit. Apparently, a second search warrant was issued for Nelson's vehicle on the basis of a substantially similar affidavit. Nelson filed a motion to suppress any and all evidence obtained by the government during the searches conducted pursuant to these warrants. Magistrate Judge Simko recommended that Nelson's motion be granted because Agent Boone's statement that "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested" was false, Agent Boone made this statement with reckless disregard for the truth, and without this statement the affidavit was insufficient to establish probable cause to search Nelson's residence and vehicle.

DISCUSSION

There is a "presumption of validity with respect to the affidavit supporting the search warrant." Franks v. Delaware, 438 U.S. 154, 171

(1978). But where the defendant "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause," then the defendant is entitled to an evidentiary hearing on the validity of the warrant. Id. at 155-56. If the defendant "proves by a preponderance of the evidence that (1) a law enforcement officer knowingly and intentionally, or with reckless disregard for the truth, included a false statement in the warrant affidavit, and (2) without the false statement, the affidavit would not have established probable cause," the search warrant must be voided and the fruits of the search must be suppressed. United States v. Neal, 528 F.3d 1069, 1072 (8th Cir. 2008) (citing Franks, 438 U.S. at 155-56). "This rationale also applies to information that the affiant deliberately or with reckless disregard for the truth omits from the affidavit such that the affidavit is misleading and insufficient to establish probable cause had the omitted information been included." Id.

A. Entitlement to Franks Hearing

Here, Magistrate Judge Simko found that Nelson was entitled to a Franks hearing because he met his preliminary burden of making a substantial showing that a false statement was intentionally or recklessly included in the affidavit and that the allegedly false statement was necessary to the finding of

probable cause. The government objects to Magistrate Judge Simko's finding that Nelson made a substantial showing that Agent Boone intentionally or recklessly included a false statement in his affidavit. The government's objection is without merit. As noted, Franks requires that a defendant challenging the validity of a search warrant make a substantial preliminary showing that a false statement was intentionally or recklessly included in the warrant affidavit. Franks, 438 U.S. at 155-56. The Franks court further explained,

> [t]o mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons.

Id. at 171.

The court finds that Nelson satisfied these requirements. Nelson attached to his motion to suppress and for a Franks hearing copies of Agent Boone's affidavit, the subpoena requesting subscriber information for IP address 216.16.82.227 from 12:29 a.m. GMT to 12:46 a.m. GMT on September 28, 2009, and Knology's response to the subpoena, containing the DHCP logs for October 6, 2009, and October 12, 2009. These documents show a one- to two-week discrepancy between the date indicated on the subpoena and the dates on the DHCP logs turned over by Knology. And Agent Boone's

affidavit explains the importance of obtaining subscriber information for an IP address for an "exact" date and time. Although the government responded to Nelson's motion by providing additional documents that may link the information provided by Knology with the information requested in the subpoena, the court finds that the documents provided by Nelson in conjunction with his motion to suppress and for a Franks hearing were sufficient to make a preliminary showing that Agent Boone recklessly and falsely stated that Knology provided information stating that Nelson subscribed to the IP address 216.16.82.227 on the dates and times requested in the subpoena. The government did not object to Magistrate Judge Simko's finding that the allegedly false statement was necessary to a finding of probable cause. Thus, the court adopts Magistrate Judge Simko's recommendation that Nelson was entitled to an evidentiary hearing on his challenge to the sufficiency of the affidavit in support of the search warrant.

B. Existence of False Statement

Considering all of the evidence at the evidentiary hearing, Magistrate Judge Simko found that Agent Boone's statement, "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested," was false. The government objects to this finding and Magistrate Judge Simko's finding that Knology did not provide any

information about the "dates and times requested" in the subpoena. The court agrees with Magistrate Judge Simko's conclusion that Agent Boone's statement was false in two respects. First, contrary to Agent Boone's statement in the affidavit that Knology responded to the subpoena by identifying the subscriber for IP address 216.16.82.227 for the "dates and times requested," Knology responded with subscriber information for this IP address for a time at least 24 hours after the times listed in the subpoena. In the subpoena, Knology was asked to produce subscriber information for IP address 216.16.82.227 for 12:29 a.m. GMT to 12:46 a.m. GMT on September 28, 2009, which converts to 7:29 p.m. CDT to 7:46 p.m. CDT on September 27, 2009. The earliest data in the DHCP logs produced by Knology in response to the subpoena is from 11:24 p.m. CDT on September 28, 2009. Thus, Agent Boone's statement that Knology responded to the affidavit with information about the subscriber "on the dates and times" requested was false.

Second, setting aside the discrepancy between the September 27, 2009, date and times listed on the subpoena and the September 28, 2009, date and times in the DHCP logs provided by Knology, Agent Boone's statement that Knology "responded with information stating" that Nelson was the subscriber on either date was false because, as Agent Boone admitted, Knology never stated that Nelson was the subscriber for IP address 216.16.82.227 on September 28, 2009. Rather, Knology's statement to Agent Boone about the

identity of the subscriber related only to October 6, 2009, and October 12, 2009: "Here is the info for the IP address '216.16.82.227' for the date of 10/06/2009. The same user is assigned the same IP address today." Exhibit 2 at 1. Knology provided DHCP logs for October 6, 2009, and October 12, 2009, with this statement. With respect to the dates before October 6, 2009, Knology stated to Agent Boone that it was unable to determine the identity of the subscriber. Indeed, on October 8, 2009, two days after the October 6, 2009, DHCP log linking IP address 216.16.82.227, computer MAC address 00:1e:ec:3e:cc:36, and modem MAC address 00:1E:46:BE:D3:EC, was available, Knology informed Agent Boone that it could not yet determine the subscriber information for IP address 216.16.82.227 and believed that the subscriber had not been online since September 28, 2009.

Thus, contrary to Agent Boone's assertion in the affidavit that ***Knology*** stated that Nelson was the subscriber on September 28, 2009, it was ***Agent Boone*** who reached this conclusion. As Agent Boone repeatedly testified, he determined the subscriber associated with the file-sharing activity on September 28, 2009, by considering the September 28, 2009, DHCP logs in Spence's October 7, 2009, email, the October 6, 2009, and October 12, 2009, DHCP logs attached to Griggs's October 12, 2009, email, and the IP history Agent Boone ran as part of his investigation. He testified that based on the consistency of the port number 22662, the modem MAC address

00:1E:46:BE:D3:EC, and the computer MAC address 00:1e:ec:2e:cc:36 through the IP history and DHCP logs for IP address 216.16.82.227, he determined that only one computer could be responsible for the file-sharing activity on this IP address. While the court does not doubt Agent Boone's sincere belief that he correctly determined the subscriber of IP address 216.16.82.227 at the relevant times, the court finds that Agent Boone's statement that Knology responded to the subpoena "with information stating that IP address 216.16.82.227 was subscribed to by [Nelson] . . . on the dates and times requested" was false. This misrepresentation as to the source of the information that Nelson was the subscriber of IP address 216.16.82.227 is a false statement under Franks. See United States v. Reinholz, 245 F.3d 765, 774 (8th Cir. 2001) (finding that misrepresentation of pharmacist who knew suspect had legally purchased iodine crystals as "confidential and reliable" source of information that the suspect was involved in the use and distribution of methamphetamine was false statement under Franks); United States v. Davis, 714 F.2d 896, (9th Cir. 1983) (finding affiant's statement that he received information directly from informants was false where affiant received the information another officer who in turn received the information from the informants).

This case is analogous to United States v. McCain, 271 F. Supp. 2d 1187, 1191 (N.D. Cal. 2003), in which the United States District Court for the Northern District of California found that an affidavit describing a wiretap as a

"confidential and reliable source" was untruthful because the language used throughout the affidavit falsely suggested that the "confidential and reliable source" was a person. For example, the officer stated that "according to the" confidential and reliable source, the suspect was involved in drug activity. Id. The court found that the affidavit contained false statements by drawing a distinction between a conclusion provided by a source and information provided by a source from which an officer derives conclusions: "While investigators might derive these conclusions from information provided by the wiretap, the wiretap itself could have presented only evidence on which the conclusions are based, not the conclusions themselves." Id. As a result, the court found that the affidavit was false in two respects: first, "it was misleading as to the source of the information presented," and second, "[the officer] . . . summarized the conversations in a manner which presented his own interpretations as direct factual evidence." Id. at 1195.

Similarly, in this case, Agent Boone misled the issuing judge by misrepresenting his own analysis and conclusion regarding the identity of the subscriber associated with the suspected file-sharing activity as a factual statement made by Knology. Knology did not definitively state the identity and address of the subscriber of IP address 216.16.82.227 on the dates and times requested in the subpoena, but rather provided DHCP logs and data on which Agent Boone drew conclusions about the identity of the subscriber at the

relevant time. Thus, like in McCain, Agent's Boone's affidavit was false in two related ways: first, it falsely stated that Knology determined that Nelson was the subscriber at the relevant times, and second, it misrepresented Agent Boone's interpretation of the DHCP logs and other relevant data as a direct factual statement by Knology.

The government argues that the statement, "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested," was not false because the truth is that Nelson was the subscriber of IP address 216.16.82.227 at the time of the file-sharing activity. The government further argues that the process and data used to make this determination should be unimportant to the court because Agent Boone's ultimate conclusion was true.

The government's argument vitiates the meaning of the Fourth Amendment. As Magistrate Judge Simko noted, the Supreme Court has stated that

> [t]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.

Johnson v. United States, 333 U.S. 10, 13-14 (1948). And as the McCain court explained,

> it is not the affiant's belief that supports probable case, but the magistrate's determination based on the facts set forth on the face of the affidavit. It is also not the post hoc presentation of evidence absent from the affidavit that will support probable cause, but what is presented to the magistrate at the time he issues the warrant.

McCain, 271 F. Supp. 2d at 1192. Thus, in this case, the Fourth Amendment required that Agent Boone present to a neutral and detached magistrate judge the data and analysis that went into the determination that Nelson was the subscriber of the suspected IP address at the relevant time so that the magistrate judge could determine whether the data and analysis constituted probable cause to support a search of Nelson's home. Contrary to the government's argument, it is not enough that Agent Boone accurately analyzed this data himself.

Further, the government's suggestion that the identity of the person or entity that determined that Nelson was the subscriber is irrelevant in light of the fact that the underlying determination was accurate is unavailing. As the Ninth Circuit has found, Franks requires a court to consider the truth or falsity of a statement that the affiant received information from a particular source, not just the truth or falsity of the information itself. See Davis, 714 F.2d at 899 (finding that district court erred in focusing on the truth or falsity of

information contained in the affidavit and ignoring the truth or falsity of the statement that the affiant received the information directly from an informant rather than from another officer). Thus, contrary to the government's assertion, the court must consider the veracity of Agent Boone's assertion that ***Knology stated*** that Nelson was the user engaged in the file-sharing activity rather than the veracity of the underlying conclusion itself.

Because Agent Boone's statement that "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested" falsely indicated that Knology determined that Nelson was the subscriber from 7:29 p.m. CST to 7:46 p.m. CST on September 27, 2009, the court adopts Magistrate Judge Simko's recommendation that this statement was false.

C. Recklessness of False Statement

Next Magistrate Judge Simko found that Agent Boone made the false statement in the above-quoted paragraph with reckless disregard for the truth. The government objects to Magistrate Judge Simko's findings that Agent Boone's assertion that it was Knology that stated the identity of the subscriber was made with reckless disregard for the truth, that Agent Boone omitted from the affidavit the fact that it was Agent Boone himself who concluded that Nelson was the subscriber on the dates and times requested with reckless

disregard for the truth, that Agent Boone had obvious reasons to doubt the accuracy of his statement that Knology responded to the subpoena with information indicating that IP address 216.16.82.227 was subscribed to by Nelson on the dates and times requested, that Agent Boone's statement rose above the level of mere negligence to the level of reckless disregard for the truth, and that attributing Agent Boone's false statement to mere negligence would obliterate a fine but important distinction drawn by the Fourth Amendment.

Courts do not require that every fact recited in an affidavit be correct. United States v. Buchanan, 574 F.3d 554, 563 (8th Cir. 2009). Indeed, "probable cause may be founded . . . upon information within the affiant's own knowledge that sometimes must be garnered hastily." Id. (internal quotation omitted). "Therefore, the affidavit must be 'truthful' in the sense that the information put forth is believed or appropriately accepted by the affiant as true." Id. (internal quotation omitted). To determine whether a statement is made with reckless disregard for the truth, courts "do not look simply at whether a statement included in the affidavit was true." Neal, 528 F.3d at 1072. Rather, the test is whether "when looking at all the evidence available to the officer, the officer 'must have entertained serious doubts as to the truth of his [or her] statements or had obvious reasons to doubt the accuracy of the information he [or she] reported." Id. (quoting United States v. Schmitz, 181

F.3d 981, 986-87 (8th Cir. 1999); see also United States v. Clapp, 46 F.3d 795, 801 n.6 (8th Cir. 1995). "A showing of negligence or innocent mistake is not enough to establish a Franks violation." Neal, 528 F.3d at 1072.

Here, the court agrees with Magistrate Judge Simko that Agent Boone did not intentionally mislead the issuing court. But the court also agrees with Magistrate Judge Simko that Agent Boone recklessly included a false statement—that Knology provided information stating that Nelson was the subscriber on the dates and times listed in the subpoena—in his affidavit because the facts show that Agent Boone had obvious reasons to doubt the accuracy this statement. Indeed, Agent Boone repeatedly testified that he, not Knology, determined that Nelson was the subscriber on September 28, 2009. When asked whether Knology told him that Nelson was the subscriber or whether Knology provided him with information from which he figured out that Knology was the subscriber, Agent Boone responded, "I used the logs, the DHCP logs [Knology] sent me, and the other information that I had in my investigation and put them together to find out that it was Jeremy Nelson at this address." Agent Boone also admitted that Knology never stated in a single sentence that Nelson subscribed to IP address 216.16.82.227 on September 28, 2009. And Agent Boone testified that he determined that Nelson was the subscriber by looking at the information provided by Knology as well as the information contained in the IP history he obtained. Notably, Agent Boone did

not testify that Knology explicitly stated that Nelson was the subscriber on September 28, 2009, or from 7:29 p.m. to 7:46 p.m. CDT on September 27, 2009, the times listed in the subpoena. Overall, Agent Boone's testimony shows that he had obvious reasons to doubt the truth of his statement that Knology stated that Nelson was the subscriber on the dates and times listed on the subpoena, and as a result the court finds that Agent Boone recklessly misled the issuing judge by misrepresenting the nature of the source of this conclusion as an affirmative statement of fact by Knology rather than as Agent Boone's analysis of the data provided by Knology. See Reinholz, 245 F.3d at 774 (finding that district court did not err in finding that officer recklessly misled magistrate judge by misrepresenting the nature of his source as confidential and reliable).

The government argues that Agent Boone's falsehood was a result of negligence or mistake, rather than reckless disregard for the truth, because the falsehood arose out of the manner in which Agent Boone phrased the statement rather than the underlying conclusion. But an examination of Agent Boone's affidavit as a whole convinces the court that Agent Boone's inclusion of the false statement was a product of more than mere negligence or innocent mistake. Agent Boone provided extensive information about peer-to-peer software, the secure hash algorithm method for identifying suspected files as child pornography, the Globally Unique Identifier number used by some peer-

to-peer software, the files he identified in the IP history for IP address 216.16.82.277, and the function and meaning of IP addresses. Agent Boone even pointed out the importance of issuing a subpoena to an internet service provider for "an exact date/time pertaining to an IP address for an investigation." Based on the detailed information Agent Boone provided in other parts of his affidavit, the court finds that Agent Boone must have entertained serious doubts as to the truth of his assertion that Knology provided information stating that Nelson was the subscriber for the dates and times requested in the subpoena when in reality, neither Knology nor Agent Boone had any data about the exact times listed in the subpoena and it was Agent Boone who concluded that Nelson was the subscriber on September 28, 2009, by analyzing the MAC addresses in the DHCP logs provided by Knology as well as the port number from the IP history Agent Boone obtained. The detail contained in other parts of Agent Boone's affidavit shows that he knew that given the nature of the investigation, detailed and precise information was required to show a link between the suspected child pornography files, an IP address, and an individual subscriber. As a result, the court finds that Agent Boone had obvious reasons to doubt the accuracy of his assertion that Knology stated that Nelson was the subscriber on the dates and times listed in the subpoena, and that this representation was not a result of mere negligence or innocent mistake.

The government also argues that if the issuing judge would have had all of the facts Agent Boone had, the issuing judge would have reached the conclusion that Nelson was the subscriber, and therefore, there can be no deliberate or reckless disregard to the truth. The government cites no authority for the proposition that there can be no deliberate or reckless disregard for the truth when the affiant possesses, but does not include in the affidavit, knowledge that would support a finding of probable cause. Indeed, the case law suggests that such omitted information cannot save an affidavit that otherwise violates Franks. The Ninth Circuit has explained that where an affiant intentionally or recklessly fails to properly identify the source of information in an affidavit, "[t]he fact that probable cause did exist and could have been established by a truthful affidavit does not cure the error." David, 714 F.2d at 899. And the Eighth Circuit has rejected the proposition that information possessed by the affiant but not included in the affidavit can overcome a Franks violation: "In any case, retroactively supplementing the affidavit with material omissions bolstering probable cause would undermine the deterrent purpose of the exclusionary rule." Reinholz, 245 F.3d at 775 (internal citation omitted). See also McCain, 271 F. Supp. 2d at 1193 ("[The affiant's] genuine belief in the overall existence of probable cause does not excuse a reckless disregard for truth in the factual assertions set forth in the affidavit upon which the magistrate's finding was based."). Thus, the fact that

an affiant possessed sufficient information to support a finding of probable cause does not preclude a finding that a statement actually included in the affidavit was made with intentional or reckless disregard of the truth. Moreover, the government's argument misses the key inquiry in this case, which is whether Agent Boone's assertion that ***Knology stated*** that Nelson was the subscriber was made with reckless disregard for the truth. The court doubts that the issuing judge would have agreed with this statement even if he had had all of the information available to Agent Boone. For these reasons, the government's argument that Agent Boone could not have been reckless because the issuing judge would have agreed that Nelson was the subscriber at the relevant times is unavailing.

Considering all of the evidence available to Agent Boone at the time he created the affidavit, the court adopts Magistrate Judge Simko's recommendation that Agent Boone included a false statement in his affidavit with reckless disregard for the truth.

The court need not consider the government's objection to Magistrate Judge Simko's finding that Agent Boone recklessly omitted from the affidavit the material fact that it was Agent Boone himself who concluded that Nelson was the subscriber on the dates and times requested because this case is properly treated as a false statement case, not an omission case. Generally, when information is deliberately or recklessly omitted from the affidavit such

that the affidavit is misleading, the court must determine whether the affidavit as supplemented by the omitted material is sufficient to establish probable cause. Jacobs, 986 F.2d at 1235. But where an affidavit includes a false statement made with reckless disregard for the truth, the court must remedy the Franks violation by deleting the false statement, not by considering the true information that was omitted from the affidavit. Reinholz, 245 F.3d at 775.

For example, in Reinholz, 245 F.3d at 774, the district court found that the affiant recklessly misled the issuing judge by claiming to have received information from a "confidential and reliable" source who had personal knowledge of the suspect's methamphetamine use and distribution when, in fact, the officer's source was a pharmacist who had dropped his request for anonymity and who knew only that the suspect purchased iodine crystals. The government argued that the court should not have deleted the paragraph containing the information from the pharmacist, but rather should have considered whether the affidavit supported a finding of probable cause when supplemented by the omitted information. Id. at 774-75. The Eighth Circuit rejected this argument, reasoning:

> [t]he district court properly deleted the misrepresentations contained in the fifth paragraph of the affidavit. [The officer's] affidavit included false statements made with reckless disregard for the truth. We remedy a Franks misrepresentation by deleting the false statements. The entire fifth paragraph of [the officer's] affidavit contains false information and the district court was correct to delete it. Thus, the district court did not err when it deleted the fifth paragraph of [the officer's] affidavit.

> We recognize that the exclusionary rule does not apply to negligent misrepresentations or omissions. In any case, retroactively supplementing the affidavit with material omissions bolstering probable cause would undermine the deterrent purpose of the exclusionary rule. Therefore, the district court did not err when it refused to supplement the affidavit with more precise information concerning the nature of [the officer's] source.

Id. at 775 (internal citations omitted).

The Eighth Circuit's approach to false statements regarding the source of information contained in an affidavit is echoed by a leading authority on the Fourth Amendment:

> [A]n affidavit with knowing falsehoods in it . . . should not be open to rehabilitation by a process of substituting for the affiant's lies other information which is really the truth from which he deliberately departed. To treat the case as an omission situation and then substitute that which was "omitted" fails to recognize that such addition to the affidavit is appropriate only as to omitted information tending to cast some doubt on the probable cause otherwise shown.

2 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 4.4 (4th ed.) (citing State v. Nielsen, 727 P.2d 188 (Utah 1986)). See also Nielsen, 727 P.2d at 196 (Stewart, J., dissenting) ("The majority refuses to set aside the officer's misstatement by characterizing the misstatement as an 'omission' which must be 'inserted' into the affidavit. The cases relied upon by the majority do not support its holding, and Franks itself requires the opposite result. . . . [T]he affiant officer in the instant case did not omit anything from the warrant affidavit. He affirmatively misstated the source of his knowledge, and the rule in Franks controls this case."); but see Nielsen, 727 P.2d at 192

n.2 (majority opinion) (finding that where affiant represented that he talked to informant personally when in fact another officer talked to the informant and relayed the information to the affiant, "it seems appropriate to analyze the affidavit for probable cause by adding the information improperly omitted"). As the Ninth Circuit explained in a case involving a misrepresentation of the identity of a source,

> [the officer] could have relied on the facts learned from his subordinates to prepare a truthful affidavit. This entire problem could have been avoided if [the officer] had simply rewritten the affidavit to indicate that he was relying on his officers who had personally interviewed the informants. Similarly, the affiant in Franks could have stated that his fellow officer interviewed the informants in question. By failing properly to identify their sources of information the affiants in each case made it impossible for the magistrate to evaluate the existence of probable cause. Franks teaches that when, as in this case, that failure is intentional the warrant must be invalidated. The fact that probable cause did exist and could have been established by a truthful affidavit does not cure the error.

Davis, 714 F.2d at 899 (internal citations omitted). Thus, in the final step of the Franks analysis, the court will delete Agent Boone's false statement and consider whether the affidavit establishes probable cause and will not consider the true information that Agent Boone omitted from the affidavit.

D. Probable Cause

In the final step of the Franks analysis, Magistrate Judge Simko recommended that because Agent Boone's statement, "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was

subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested," was false and made with reckless disregard for the truth, the statement should be excised from the affidavit, rendering the affidavit insufficient to establish probable cause to search Nelson's home. The government objects to Magistrate Judge Simko's recommendations that the affidavit lacked probable cause for the issuance of a search warrant and that the evidence obtained pursuant to the search warrant should be suppressed.

When an affidavit includes a false statement made with reckless disregard for the truth, the court must delete the false statement and determine whether the remaining information in the affidavit is sufficient to support a finding of probable cause. Neal, 528 F.3d at 1072; Reinholz, 245 F.3d at 775. "An affidavit establishes probable cause for a warrant if it sets forth sufficient facts to establish that there is a fair probability that contraband or evidence of criminal activity will be found in the particular place to be searched." United States v. Snyder, 511 F.3d 813, 817 (8th Cir. 2008). (internal quotations omitted). The affidavit must include sufficient information to allow the issuing judge "to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." Illinois v. Gates, 462 U.S. 213, 239 (1983).

Here, Agent Boone included in the affidavit the false information that Knology stated that Nelson was the subscriber on the dates and times listed on

the subpoena, and this is the information that must be excised from the affidavit. See Neal, 528 F.3d at 1072. Thus, the statement, "[o]n October 12, 2009, Knology responded with information stating that IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078 on the dates and times requested," now reads, "IP address 216.16.82.227 was subscribed to by JEREMY NELSON at 616 ½ Locust St, Yankton, SD 57078." The court agrees with Magistrate Judge Simko that the affidavit as modified does not establish probable cause to search Nelson's home or vehicle. Indeed, the modified paragraph is the only paragraph in the affidavit linking the suspected file-sharing activity with Nelson and his residence. And as modified, this paragraph contains only a bare conclusion that Nelson subscribed to the IP address associated with the suspicious file-sharing activity. This bare conclusion does not provide sufficient information to allow a magistrate judge to determine whether there is a fair probability that evidence of possession or distribution of child pornography will be found in Nelson's home. Thus, the affidavit lacks probable cause to support a search of Nelson's residence, and the search warrant must be voided and the fruits of the search must be suppressed. See Neal, 528 F.3d at 1072; see also United States v. Strauser, 247 F. Supp. 2d 1135, 1144-45 (E.D. Mo. 2003) (granting motion to suppress where warrant application lacked sufficient link between the defendant and the distribution of child pornography).

Despite Agent Boone's sincere belief that he accurately determined and stated in the affidavit the identify of the subscriber of the IP address engaging in distribution of child pornography, he recklessly misrepresented the source of this conclusion and made it impossible for the issuing judge to determine whether there was probable cause to search Nelson's home. Without this false statement, Agent Boone's affidavit does not establish probable cause to search Nelson's home or vehicle, and as a result, it is

ORDERED that the court adopts the Report and Recommendation of Magistrate Judge Simko (Docket 27) as supplemented herein, and therefore, Nelson's motion to suppress evidence and request for a Franks hearing (Docket 17) is granted.

Dated July 12, 2010.

BY THE COURT:

/s/ *Karen E. Schreier*
KAREN E. SCHREIER
CHIEF JUDGE